==========
H I P A A n o t e -- Volume 2, Number 34 – September 4, 2002

>>From Phoenix Health Systems--HIPAA Knowledge--HIPAA Solutions<<
=>Healthcare IT Consulting & Outsourcing<=
==========

PUTTING THE PRIVACY CHANGES TO WORK:
A "How-To" Guide to the August 2002 HIPAA Privacy Rule Modifications
60-minute audio conference + slides

** Wednesday, September 25 at 2:00 PM **

For more information or to register, go to:
http://www.HIPAAdvisory.com/ezcart/index.cfm

==========

This week's HIPAAnote...

*** HIPAA Access Control Requirements:
Traditional Password Security vs. Technology-based Solutions ***

Similar to their Y2K efforts, healthcare organizations have the opportunity to investigate many alternatives that will help them comply with the proposed HIPAA Security provisions. In the area of Access Control requirements, technology-driven access control alternatives such as smart cards or biometrics may make more sense for some organizations than going the route of implementing more stringent, traditional password security policies and procedures.

Why? Traditional password security is becoming increasingly cumbersome. Most computer users work within a proliferation of passwords for accessing operating systems, networks, email applications, online banking, ATMs, calling cards, and cell phones. Most healthcare employees have at least two different passwords for their computer systems. The multiplicity of passwords has made the management of passwords more complex.

Typically, you will find three general categories of password management practiced in healthcare:

1. passwords automatically generated by the computer system within a pre-defined interval,
2. passwords generated by the computer user when the user is required to generate a password, or
3. passwords generated upon beginning of employment and never changed.

All three approaches have negatives. While system-generated passwords are usually stronger than user-selected passwords, they are harder to remember and are frequently written down -- a security "no-no". When a password is not

remembered, the result can be serious inconvenience and operations delays as well as information systems (IS) staff intervention. User-generated passwords, on the other hand, are typically easy to remember, but, as a result, are easy targets for malicious users or skilled hackers. Passwords generated once and never changed are particularly easy targets for malicious users and skilled hackers.

An average hospital has about 1,200 computer users. Currently, most hospitals do not have a policy that requires the system or the user to change passwords periodically. With this relaxed password management practice, an average IS department still receives an estimate of 50 to 60 password calls each month. Using the Gartner Group's numbers, resetting passwords is minimally costing a hospital $700 to $1,680 per month. Undoubtedly, this cost will double to triple when hospitals begin to implement stringent password policy to comply with HIPAA security standards. Further, implementing more stringent password practices within a healthcare facility will add new stress and frustration to both staff and physician.

Technology solutions such as badge readers, smart cards or biometrics can offer covered entities viable alternatives to implementing more stringent password management controls. The costs of deploying such technology-driven protections vary from $40 to over $200 a workstation. While these alternatives may require extra up-front research, planning and deployment efforts -- plus higher up-front expenditures –- long-term benefits may very well justify the investment.

At a minimum, larger covered entities should investigate using such technology-based solutions within their organization. A final tip: if you pursue this route, start out with a small pilot program within a controlled environment. This approach will provide real-world data based on your organization's specific environment, to help you assess which alternatives will meet your short- and long-term needs most cost-effectively.

Josef Spencer, Director
Phoenix Health Systems

For more...

* on the HIPAA security standards, go to:
http://www.hipaadvisory.com/regs/securityandelectronicsign/

* technology-related information, go to:
http://www.hipaadvisory.com/tech/

That's today's HIPAAnote...now, pass it along!

==========

Bring your HIPAA questions and ideas to life at... HIPAAlive!

Join nearly 5,000 other thinkers, planners, learners and lurkers who are already members of our sister email discussion list. We almost make HIPAA fun! Almost. (Also available in a PREMIUM version of easy-to-navigate, individually formatted, "cleaned up" digests.) Now when you join HIPAAlive-Premium, you receive a FREE Doc Site Membership!

Find out more about HIPAAlive, the Doc Site, and HIPAAlive-Premium at:
http://www.HIPAAdvisory.com/live

==========
==========

HIPAAnotes are published weekly as a learning tool to help you and your associates stay tuned-in to HIPAA and its implications. Forward it to anyone with a "need to know" through your own internal mailing list, intranet or newsletter -- whatever works for you...

Our HIPAAcratic oath: We'll use your ideas for HIPAAnotes -- send them!
Email D'Arcy Gue, Editor: info@phoenixhealth.com

==========
=
You are currently subscribed to hipaanotes as: kmckinst@dmhhq.state.ca.us

To unsubscribe, send an email to: leave-hipaanotes-16283428V@lists.hipaalert.com
---
List archives:
http://www.hipaadvisory.com/notes/archives.htm
==========
=